IN THE CLAIMS:

1-16. (Canceled)

17. (Previously Presented) A method of authenticating a client with a server across a network connection, comprising the steps of:

requesting, by the client, access to the server by sending a first set of values to the server, wherein the first set of values includes a client-generated random value, a large prime number, a primitive root of the large prime number, and the primitive root raised to a power of a large random integer less than the large prime number minus one;

responding, by the server, to the client by generating a one-time challenge token that depends on at least a server-generated random value and sending the challenge token to the client, wherein the server generates the challenge token by exclusive-oring the server-generated random value with a first hash, and wherein the first hash is a hash of the primitive root of the large prime number raised to a power, a digest of the client's userid and password, and the client-generated random value;

retrieving, by the client, the server-generated random value from the challenge token;

sending, by the client, the server-generated random value and a userid of the client to the server;

verifying, by the server, the received server-generated random value from the client is correct by comparing the server-generated random value received from the client with the server's stored value of the server-generated random number;

if the server-generated random value from the client is verified by the server, generating a one-time authentication token by the server;

sending, by the server, the one-time authentication token to the client to thereby give the client permission to access the server;

verifying, by the client, the validity of the one-time authentication token received from the server;

if the client verifies that the one-time authentication token from the server is valid, changing, by the client, the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result;

sending, by the client, the result, the userid, and the message authentication code to the server;

retrieving, by the server, the new digest by exclusive-oring the mask with the received result;

verifying, by the server, the received message authentication code; and

if the received message authentication code is verified, changing, by the server, the client password by replacing a digest of at least the old password with a digest of at least the new password.

18-24. (Canceled)